

Re: where is it hiding?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2005-04/0173.html>

From: Wade A. Hilmo [MS] (wadeh_at_microsoft.com)

Date: 04/18/05

Date: Mon, 18 Apr 2005 14:19:56 -0700

I am not sure that I understand what you are saying.

IIS always loads the registered filters before it starts processing requests. And it doesn't unload filters until it is shutting down the host process and has reached the point where no new requests are accepted, and all existing requests have completed. If a filter is properly registered and can be loaded, there is no window of time where a request can be processed without the filter loaded.

The messages that you see in the UrlScan log are just there to indicate when it is loaded and unloaded. Whenever UrlScan loads, it will put a line in the log file indicating that it is initializing. Whenever UrlScan is unloaded, it will put a line in the log file indicating that it is terminating.

Assuming that a filter is properly installed, it is possible for IIS to fail to load it. Such a failure can occur in 3 places: The operating system can fail to load the filter prior to calling any entry points (due to insufficient memory, ACL problems, file not found, dependency dll not found, etc.) The operating system can load the filter and call into the DllMain function and the DllMain function can fail, in which case the OS will unload the filter and fail the LoadLibrary call back to IIS. Finally, the OS might successfully load the filter, but the filter can fail it's GetFilterVersion entry point, in which case IIS will fail the attempt to load the filter.

In all of these cases, IIS will create an event in the event log indicating the failure and error code. In IIS 6's default configuration, any failure to load a filter will cause the worker process to shut down before taking any requests. In IIS 5.1 and earlier, IIS will take requests even if a filter fails to load (but there is nothing that UrlScan can do about this.)

UrlScan does not export a DllMain entry point, and it's GetFilterVersion function has no code paths that can return a failure. Because of this, the only reason that IIS can fail to load a properly registered UrlScan is if the operating system itself fails to load the dll into memory.

Based on all of the above, there are only two ways that IIS can ever take a request that UrlScan doesn't see. First is that UrlScan is not properly

microsoft.public.inetsrvr.iis.security: Re: where is it hiding?

installed (or is not installed as a global filter, which is the only supported configuration.) Second, this can happen if the OS fails to load UrlScan for some reason outside of IIS or UrlScan's direct control and you are running IIS 5.1 or earlier. In the latter case, there will be entries in Event Viewer that show the filter load failures.

If you can give a better description of **exactly** what you are seeing, then perhaps I can come up with a more direct explanation.

Thank you,
–Wade A. Hilmo,
–Microsoft

"Advertiser" <advertiser@VideoClassified.com> wrote in message news:4263f899\$1_2@127.0.0.1...

> *I see nothing wrong with IIS gracefully shutting down one of ISAPI DLLs after a configurable period of inactivity. The problem that I had was that after such gracefull shutdown UrlScan stopped filtering off .exe .dll requests configured in its INI file. This happend when I installed UrlScan for the first time. I've added .exe and .dll to the list of prohibited extensions and changed directory of its log file. I didn restart IIS. Once I've made sure that .exe and .dll requests reach IIS, I've uninstalled UrlScan from the control panel and installed it again. I've also restarted IIS couple of times and so far UrlScan has been filtering out evrything*
I've
> *configured it to, even after several gracefull termination and restarts that*
> *happened without my intervention.*
>
> *So the problem doesn't seem to be gone, its just hiding somewhere. And I'd appreciate any information that would explain why UrlScan didn't restart after first gracefull shutdown and what can I do to prevent it in the future.*

> Thanks.

> "Wade A. Hilmo [MS]" <wadeh@microsoft.com> wrote in message news:OkbN%23dDRFHA.996@TK2MSFTNGP09.phx.gbl...

> Hello,

>>

> > *UrlScan only writes the termination entry in the log when it is gracefully*

> > *unloaded by IIS. This only happens when the web service shuts down (or in*

> > *the case of IIS 6, when the hosting worker process shuts down.)*

>>

> > *This is a normal log entry and does not generally indicate a problem.*

>>

> > Thank you,

> > –Wade A. Hilmo,

> > –Microsoft

Re: where is it hiding?

microsoft.public.inetsrvr.iis.security: Re: where is it hiding?

> >
> > "Advertiser" <advertiser@VideoClassified.com> wrote in message
> > news:42612b80\$1_2@127.0.0.1...
> > Hi there.
> > I've just installed UrlScan.dll and noticed that at the end of the log
> > that
> > it is terminated.
> > I have several questions:
> > 1) What causes termination of a UrlScan.dll?
> > 2) What should I do to prevent termination of UrlScan.dll in the future?
> >
> > Thanks.
> >
> >
> >
> >
> >
> > ===== Posted via Newsfeeds.Com – Unlimited–Uncensored–Secure Usenet
News=====
> > <http://www.newsfeeds.com> The #1 Newsgroup Service in the World! 120,000+
Newsgroups
> > ===== East and West–Coast Server Farms – Total Privacy via Encryption
=====